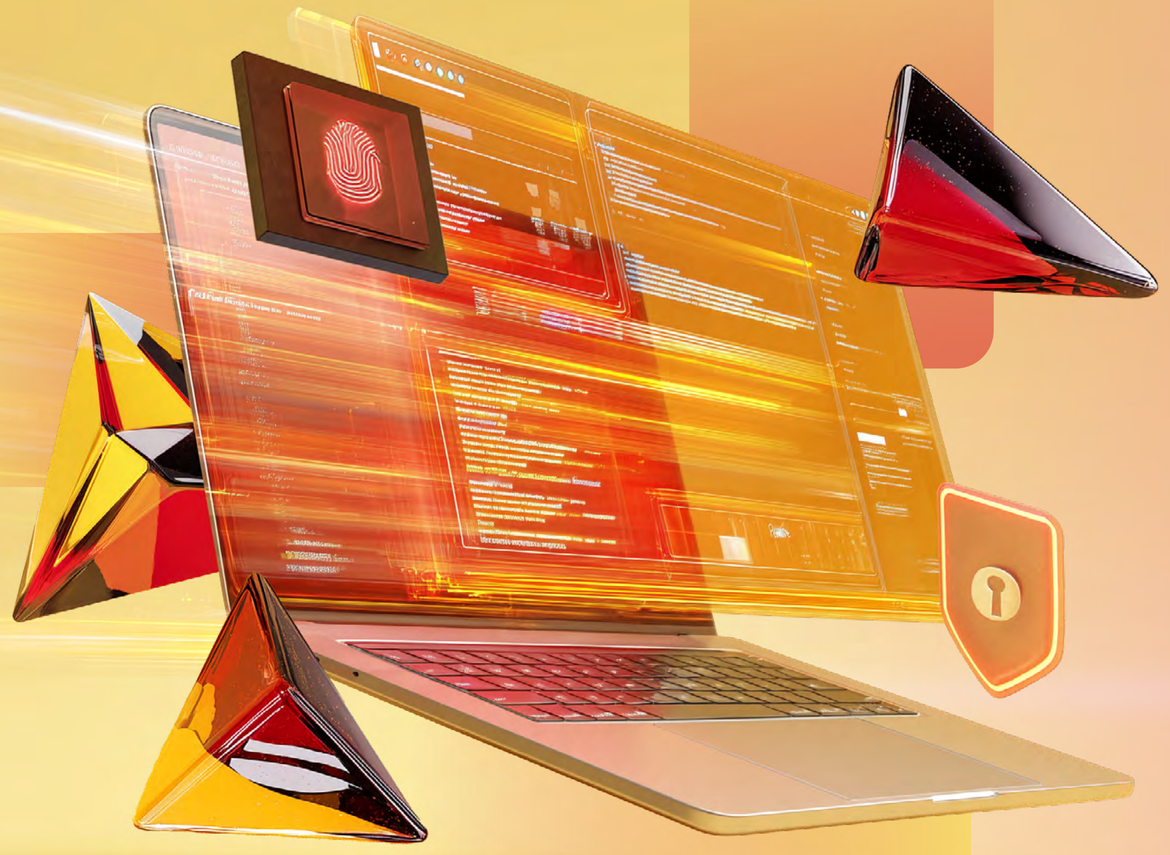
Cybersecurity

Auteurs
Anna Gerasymenko (Universiteit Leiden), **Martine Groen** (Hogeschool Utrecht),
Mick Deben (MBO Digitaal), **Rob Gerritsen** (voorheen Graafschap College),
Nicole van der Meulen (SURF)



1. Opkomend dual-use van AI in cybersecurity
2. Toegankelijkere privacyverhogende technologieën voor datadeling
3. Toenemende druk om voorbereid te zijn op post-quantumcryptografie
4. Opkomst van maatregelen voor veilige internet-of-things-omgevingen
5. Het groeiende belang van beveiligingsprotocollen voor het werken in de cloud

Inleiding

Het gebied van cyberveiligheid (cybersecurity) heeft een enorme ontwikkeling doorgemaakt sinds computerprogrammeur Bob Thomas in 1971 het Creeper-virus creëerde. Hoewel dit virus, dat gericht was op het Advanced Research Projects Agency Network (ARPANET), geen kwaadaardig virus was, markeerde het een belangrijk moment in de geschiedenis van cyberveiligheid. Meer dan 50 jaar later zijn cyberaanvallen steeds kwaadaardiger geworden en vormen ze een aanzienlijke bedreiging voor de samenleving.

Technologieën zoals artificial intelligence (AI) en internet-of-things (IoT) brengen nieuwe uitdagingen en risico's met zich mee die moeten worden aangepakt om een robuuste cybersecurity te behouden. AI kan bijvoorbeeld helpen om de verdediging tegen cyberaanvallen te verbeteren, maar kan ook de dreiging vergroten door geautomatiseerde malware mogelijk te maken.

Hoewel deze digitale technologieën organisaties blootstellen aan nieuwe bedreigingen, worden ze ook steeds essentiëler voor organisaties om zichzelf te beheren en te beschermen. Zo zal quantumcomputing de implementatie van complexe en potentieel zeer veilige cyberbeveiligingsprotocollen mogelijk maken. Dergelijke technologieën bieden aanzienlijke kansen voor zowel individuen als organisaties.

Ondanks deze technologische vooruitgang blijft het cruciaal om waakzaam te blijven voor mogelijke bedreigingen. Inzicht in de tools en technieken die cybercriminelen gebruiken en weten hoe je jezelf en je organisatie kunt beveiligen, zijn essentieel voor het behoud van (cyber)weerbaarheid. De afgelopen jaren hebben incidenten binnen de onderwijssector duidelijk gemaakt welke aanzienlijke schade kan ontstaan door een ogenschijnlijk onschuldige klik van een zogenaamde ‘patient zero’ (eerste besmette persoon/computer die de aanval verspreidt).

Het is essentieel om te begrijpen hoe technologieën de toekomst van cybersecurity kunnen en zouden kunnen vormgeven. Daarom is dit hoofdstuk opgenomen in het SURF Tech Trends-rapport om uit te leggen hoe nieuwe bedreigingen ontstaan en om de kansen te benadrukken die voortvloeien uit technologieën die niet meer weg te denken zijn uit het dagelijks leven.

Naarmate de samenleving steeds afhankelijker wordt van digitale systemen, zijn cybersecurity en cyberweerbaarheid essentiële onderdelen geworden van de strategie en bedrijfsvoering van organisaties. Het is voor organisaties essentieel om (gevoelige) data te beschermen, te voldoen aan verandere-rende wet- en regelgeving (zoals de EU Cyber Resilience Act), IoT-kwetsbaarheden tegen aanvallen of ongeautoriseerde toegang aan te pakken en cyberbedreigingen te mitigeren.

Bijdragers
Zeki Erkin (TU Delft), **Jeroen van der Ham - de Vos** (Universiteit Twente)

TREND #1

Opkomend dual-use van AI in cybersecurity

Publieke waarden

Autonomie	Privacy
Rechtvaardigheid	Integriteit | Rekenschap | Transparantie
Menselijkheid	Veiligheid

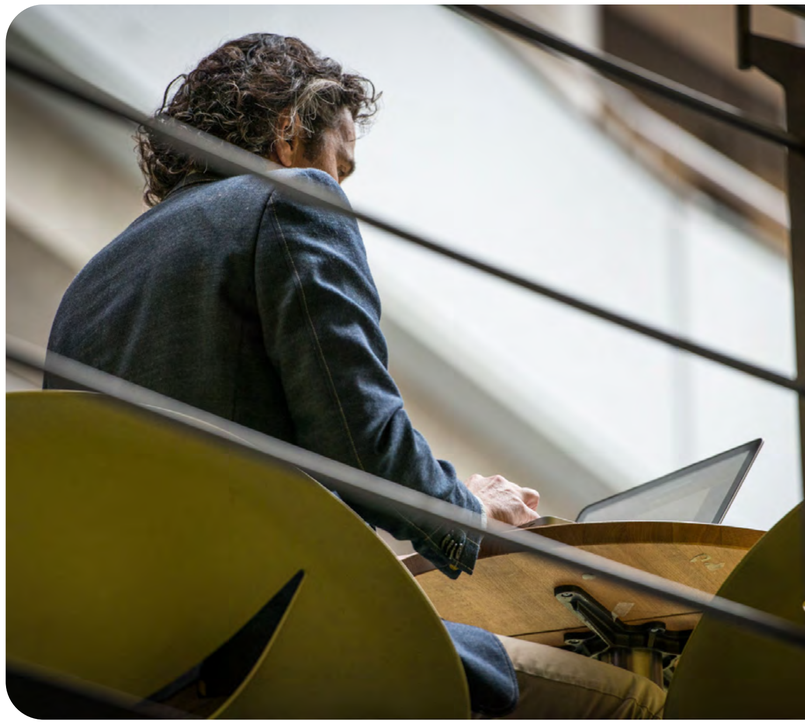
Volwassenheid WATCH PLAN **ACT**

Drivers

Automatisering en AI; Cybersecurity en vertrouwen; Technologische vooruitgang en computation; Belang van kennis en vaardigheden; Politieke/strategische inzet van kennis; Digitale transformatie

AI verandert cybersecurity door realtime detectie van bedreigingen te verbeteren en efficiënte reacties op deze bedreigingen mogelijk te maken. AI-modellen kunnen grote datasets en datastromen analyseren, afwijkingen identificeren en aanvallen voorspellen, waardoor ze een cruciaal hulpmiddel zijn voor beveiligingsactiviteiten.

Cybercriminelen maken echter ook gebruik van AI om hun aanvallen te verbeteren. Technieken zoals AI-gestuurde phishing, deepfakes en geautomatiseerde kwetsbaarheidsscans maken cyberaanvallen impactvoller en schaalbaarder. Steeds meer zorgen richten zich op de recente ontwikkelingen bij het inzetten van GenAI voor het automatisch genereren van malware met minimale input. Ook is er bezorgdheid over adversarial machine learning. Daarbij manipuleren aanvallers data om AI-modellen die gebruikt worden voor de cyberverdediging te misleiden, waardoor de modellen bedreigingen over het hoofd zien.



SIGNALEN

Opkomst van offensieve AI-mogelijkheden

Cybercriminelen maken gebruik van grote taalmodellen om contextspecifieke phishing-content en social engineering-scripts te creëren.

- **Phishing en social engineering in het tijdperk van LLM's** (link.springer.com)
- **Terug naar de hype: een update over hoe cybercriminelen GenAI gebruiken** (ibm.com)
- **Met generatieve AI wordt social engineering gevaarlijker en moeilijker te herkennen** (ibm.com)
- **Kunnen cyberaanvallen 'de lichten doven' in Europa?** (knowbe4.com)

Door AI gegenereerde deepfakes worden steeds vaker gebruikt bij identiteitsfraude en desinformatiecampagnes.

- **Hoe deepfakes, desinformatie en AI verzekeringsfraude versterken** (swissre.com)
- **Een pro-Russische desinformatiecampagne maakt gebruik van gratis AI-tools om een 'explosie van content' te stimuleren** (wired.com)
- **De donkere kant van AI: hoe deepfakes en desinformatie een miljardenrisico voor bedrijven worden** (forbes.com)

> ***"Je ziet dat AI zowel aanvallers als verdedigers kan helpen op het gebied van cybersecurity. Maar de belangrijkste focus blijft liggen op het goed uitvoeren van de basisprincipes wat betreft cyberbeveiliging en -weerbaarheid, waarbij AI een hulpmiddel is."***
>
> **- Jeroen van der Ham - de Vos,** Universiteit Twente

Open source generatieve modellen stellen actoren met beperkte middelen in staat om moeilijk detecteerbare malware te creëren en aanvallen te automatiseren.

- **Voorspelling voor open source-beveiliging in 2025: AI, overheidsinstanties en toeleveringsketens** (openssf.org)
- **OpenAI bevestigt dat cybercriminelen ChatGPT gebruiken om malware te schrijven** (bleepingcomputer.com)
- **Hoe generatieve AI de werkwijze van cybercriminele bendes verandert** (bugcrowd.com)

SIGNALEN

Defensieve AI-integratie in cyberbeveiligingsoperaties

AI-aangedreven Security Operations Centres (SOC's) gebruiken machine learning om dreigingsdetectie te automatiseren, alarmmoeheid te verminderen en incidentrespons te versnellen.

- **IBM Security, rapport over de kosten van een datalek** (cloudfront.net)
- **Microsoft Security Copilot-inzichten** (microsoft.com)

Gedragsanalyses en voorspellende AI-modellen identificeren afwijkingen en voorkomen bedreigingen voordat deze escaleren tot aanvallen (van welke omvang dan ook).

- **SOC's transformeren met AI: van reactieve naar proactieve beveiliging** (cloudsecurityalliance.org)

Network & Extended Detection and Response (NXR/XDR) platforms integreren AI om realtime correlatie van aanvallen, autonome triage en adaptieve verdediging te bieden.

- **Microsoft - Wat is uitgebreide detectie en respons (XDR)?** (microsoft.com)
- **Vectra.ai** (vectra.ai)

Risico's van vijandige AI beperken

Cyberverdedigers gebruiken tegenaanvalstraining en robuuste modelafstemming om AI-systemen beter bestand te maken tegen manipulatie en kwaadaardige invoer.

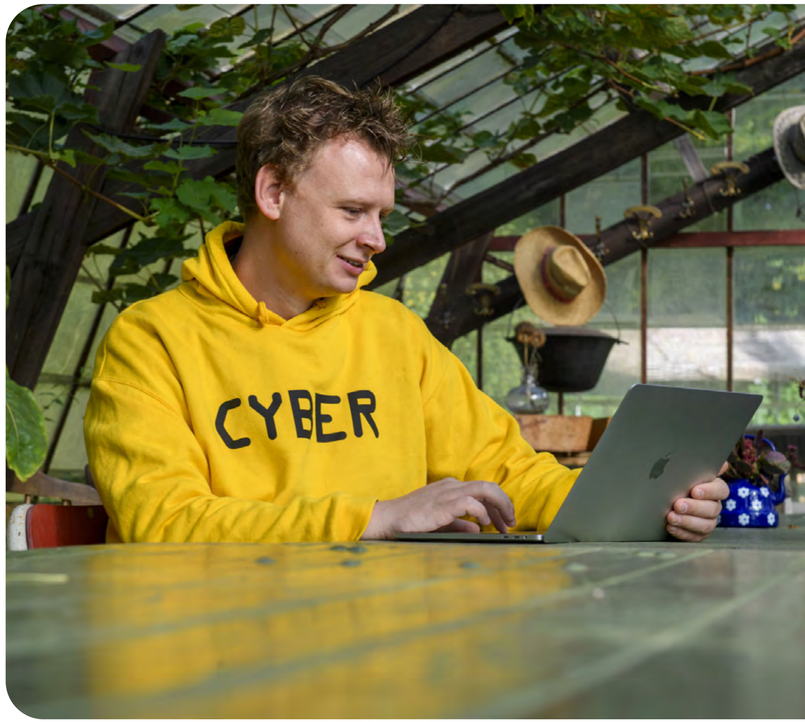
- **NIST AI-risicobeheerkader** (nist.gov)
- **MITRE ATLAS Framework** (atlas.mitre.org)

AI-red teaming en model auditing worden steeds vaker toegepast om kwetsbaarheden in machine learning-pijplijnen te identificeren voordat aanvallers hiervan misbruik kunnen maken.

- **Anthropic: uitdagingen bij red teaming** (anthropic.com)
- **Microsoft Red Team** (learn.microsoft.com)

Threat intelligence-platforms bevatten nu AI-detectiemodules om synthetische media, vervalst gedrag en gemanipuleerde datasets te signaleren.

- **Recorded Future** (recordedfuture)
- **Darktrace** (darktrace.com)
- **TNO en Jungle AI werken samen om cyberaanvallen op windturbines op te sporen en de detectiemogelijkheden te verbeteren** (tno.nl)



IMPACT

Onderwijs

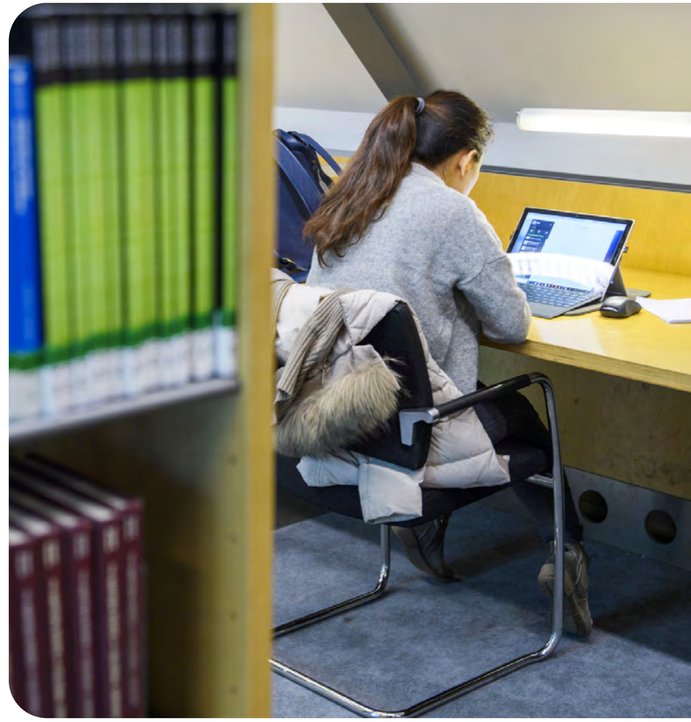
AI-tools bieden de mogelijkheid om online leeromgevingen te beveiligen door middel van anomaliedetectie en gedragsanalyse. Misbruik van AI kan echter de integriteit van het onderwijs ondermijnen door middel van geautomatiseerd spieken, deepfakes of phishing. Om AI in het onderwijs te beveiligen, moet een evenwicht worden gevonden tussen innovatie en ethische en wettelijke waarborgen.

Onderzoek

Onderzoeksinstellingen profiteren van AI voor geavanceerde dreigingsmodellering, gegevensbescherming en netwerkmonitoring. Open access-beleid en samenwerkingsverbanden op onderzoeksgebied vergroten echter ook de blootstelling aan AI-gedreven dreigingen. Robuust modelbeheer en weerbaarheid tegen vijandige acties zijn essentieel voor het behoud van de integriteit van onderzoek.

Operations

Naarmate instellingen digitaliseren, verbetert de integratie van AI in de cyberbeveiligingsinfrastructuur de real-time respons en vermindert de afhankelijkheid van handmatig toezicht. Maar AI-systemen worden dan zelf ook waardevolle doelwitten. Instellingen moeten veilige AI-pijplijnen bouwen en investeren in op bedreigingen gebaseerde AI-implementatiestrategieën om de operationele veiligheid op lange termijn te waarborgen.



TREND #2

Toegankelijkere privacyverhogende technologieën voor datadeling

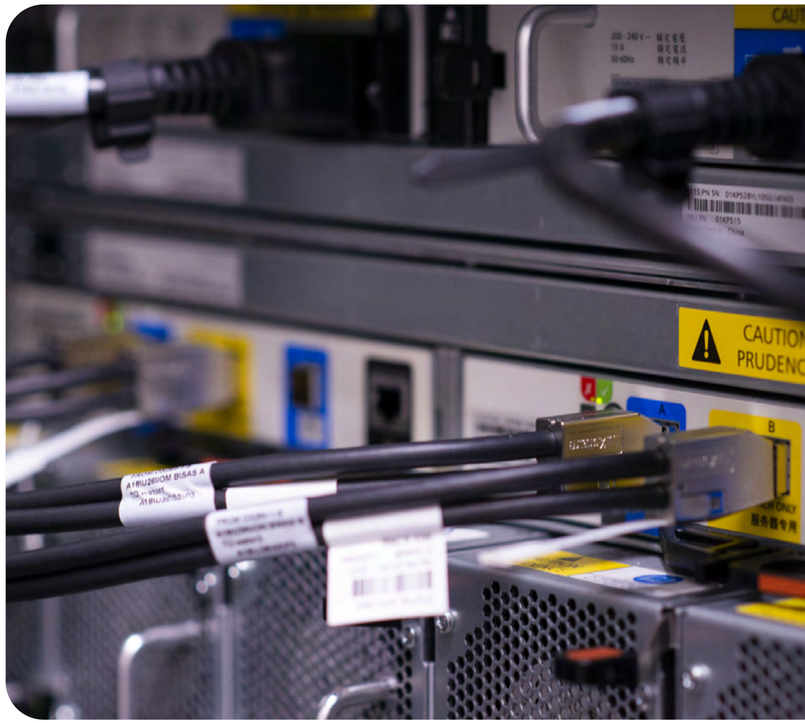
Publieke waarden

Autonomie	Privacy
Rechtvaardigheid	Integriteit | Gelijkwaardigheid | Transparantie | Rekenschap
Menselijkheid	

Volwassenheid WATCH PLAN **ACT**

Drivers

Compliance en regelgeving: Cybersecurity en vertrouwen; Automatisering en AI; Individualisering en empowerment; Digitale transformatie; Belang van kennis en vaardigheden



Privacyverhogende technologieën (privacy-enhancing technologies; PET's) beschermen gevoelige informatie en maken tegelijkertijd veilige gegevensverwerking en -uitwisseling mogelijk. De inzet van PET's – zoals differentiële privacy, synthetische datasets die lijken op echte gevoelige gegevens, federatief leren en homomorfe encryptie – wordt gestimuleerd door de groeiende vraag naar data in het onderwijs en onderzoek en vanwege de persoonlijke en vertrouwelijke aard van bepaalde data.

De recente beschikbaarheid van sectorspecifieke oplossingen hebben PET's beter toegankelijk gemaakt. Daarmee ontstaat ruimte voor privacygerichte datadeling en data-analyse tussen meerdere partijen via onderzoeksinitiatieven en publiek-private samenwerkingen.

Door PET's in IT-architecturen te integreren, worden traditionele security-by-design-benaderingen aangevuld met datacentrische controles, waardoor de kwetsbaarheid van organisaties wordt verminderd en ongeoorloofde toegang wordt tegengegaan.

SIGNALEN

Groei van oplossingen voor synthetische data

Information systems audit and control association (ISACA) (isaca.org)

Onderzoekers aan de Erasmus Universiteit worden aangemoedigd om gebruik te maken van AI-gestuurde synthetische data die wordt gegenereerd door Syntho Engine (2023) (syntho.ai)

De Universiteit Utrecht heeft het MetaSyn-platform ontwikkeld voor geanonimiseerde en FAIR-gegevenspublicatie (uu.nl)

Dienst Uitvoering Onderwijs (DUO) heeft synthetische datasets gedeeld met Nederlandse onderzoekers om onderzoeksmodellen te trainen en het onderwijssysteem te helpen verbeteren (duo.nl)

TNO PET Lab heeft als doel het gebruik van PET's in innovatie te faciliteren en te verspreiden (tno.nl)

Federatieve en veilige proefprojecten voor data-analyse

SPATIAL (TU Delft) gaat PET's integreren om betrouwbare, transparante en verklaarbare AI-oplossingen voor cyberbeveiliging te realiseren (spatial-h2020.eu)

Het Amsterdam University Medical Centre past Federated Analytics toe om gezamenlijk voorspellende modellen voor IC-uitkomsten te ontwikkelen (amc.nl)

In Nederland onderzoeken de Sociale Verzekeringsbank (SVB) en het Uitvoeringsinstituut Werknemersverzekeringen (UWV) met succes Multi-Party Computation (MPC) bij het Nationaal Innovatiecentrum voor Privacyversterkende Technologieën (NICPET) (tno.nl)

PET's bij grensoverschrijdende gegevensuitwisseling

Oproep tot federatieve infrastructuur voor gegevens van intensive care-afdelingen in heel Europa (doi.org)

EU Safe-DEED-consortiumproject gaat PET's aanbieden voor datamarkten

- eurecat.org
- tudelft.nl)

Nederlands HERACLES-project legt basis voor veilige uitwisseling van gegevens tussen de publieke en private sector in de gezondheidszorg (tno.nl)

IMPACT

Onderwijs

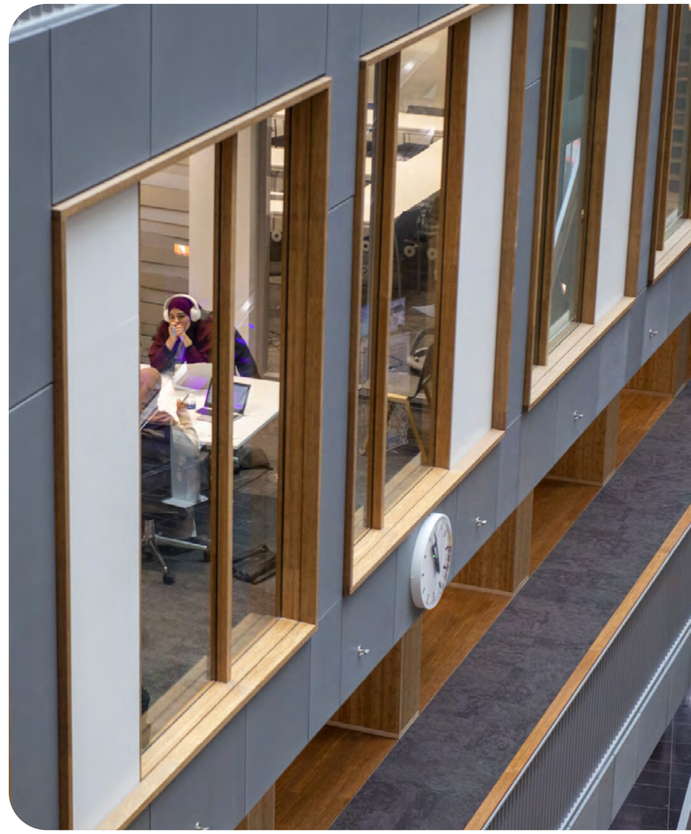
Naarmate het onderwijs digitaliseert, zullen PET's cruciaal worden voor het beveiligen van data van studenten en medewerkers in online leeromgevingen. Met behulp van cryptografische technieken en federatief leren pakken PET's privacy- en veiligheidsproblemen in leeranalyses aan, verminderen ze risico's en bevorderen ze het vertrouwen tussen studenten en docenten in adaptieve, datagestuurde of gepersonaliseerde onderwijssystemen.

Onderzoek

PET's bieden onderzoekers veilige toegang tot gevoelige of verspreide datasets, waardoor privacy-, reputatie- en strategische risico's in verband met het delen van data worden beperkt. Hoewel deze technologieën meer vertrouwen in innovatief onderzoek beloven, verhogen ze ook de druk op instellingen om deze te faciliteren vanuit de ondersteunende IT-infrastructuur.

Operations

Naarmate onderwijsinstellingen opkomende technologieën (zoals AI en edge computing) en meer volwassen technologieën (zoals cloudcomputing) adopteren, neemt de behoefte aan robuust digitaal vertrouwen en datagerichte beveiliging toe. PET's zullen essentieel worden voor het realiseren van betrouwbare en transparante beveiligingsoplossingen, die bepalend zijn voor de toekomstige IT-beveiliging en naleving van regelgeving. De volwassenheid en interoperabiliteit van PET's zullen de sectorbrede implementatie ondersteunen.



TREND #3

Toenemende druk om voorbereid te zijn op post-quantum-cryptografie

Publieke waarden

Autonomie	Privacy
Rechtvaardigheid	Integriteit | Rekenschap | Duurzaamheid
Menselijkheid	Veiligheid

Volwassenheid WATCH PLAN **ACT**

Drivers

Technologische vooruitgang en computation; Cybersecurity en vertrouwen; Automatisering en AI; Regelgeving en naleving (compliance); Kritieke infrastructuur; Digitale transformatie

Zodra quantumcomputers voldoende schaalgrootte hebben bereikt, zullen traditionele cryptografische systemen, die worden gebruikt in digitale handtekeningen en beveiligde communicatie, uiterst kwetsbaar zijn voor aanvallen.

Veel van onze huidige infrastructuren missen crypto-agility (adaptief cryptografiebeleid). Dit vertraagt de overgang naar robuuste cryptografische systemen en leidt tot blootstelling aan store now–decrypt later-dreigingen (‘nu opslaan en later ontsleutelen’). De meeste organisaties zijn of zullen aan deze decryptiedreigingen worden blootgesteld. De gereedheid van hun gegevens- en communicatiebescherming hangt af van de adoptie van post-quantumcryptografie (PQC).

Momenteel heeft het Amerikaanse agentschap NIST standaarden voor PQC-encryptie gepubliceerd en moedigt systeembeheerders aan om deze zo snel mogelijk te overwegen en toe te passen. Daarnaast streven Europese initiatieven zoals de European Quantum Communication Infrastructure (EuroQCI) ernaar om veilige communicatienetwerken op te zetten met behulp van quantum key distribution (QKD), waardoor de distributie van cryptografische sleutels mogelijk wordt gemaakt en versneld.

SIGNALEN

Standaardisatie van post-quantum-cryptografie

NIST publiceert de eerste drie definitieve standaarden op het vlak van post-quantum encryptie (nist.gov)

NIST standaardiseert quantumveilige cryptografiemethoden (cwi.nl)

Strategie 'Nu opslaan, later ontsleutelen'

Overheidsinstanties verzamelen nu al versleutelde data om die later met quantumcomputers te ontsleutelen, als onderdeel van de aanpak 'nu opslaan, later ontsleutelen' (enisa.europa.eu)

Quantumbeveiligingsinitiatieven van de nationale overheid

Het Nationaal Cyber Security Centrum (NCSC) en de AIVD nemen het voortouw bij het voorbereiden van organisaties op quantumdreigingen, door advies te geven over het in kaart brengen van het gebruik van encryptie en de overgang naar quantumveilige technologieën (ncsc.nl)

Volgende stappen National Cyber Security Centre (VK): Voorbereiding op post-quantumcryptografie (ncsc.gov.uk)

EuroQCI-project: bouwen aan quantum-veilige communicatie

Het project European Quantum Communication Infrastructure (EuroQCI) heeft tot doel een veilig communicatienetwerk in heel Europa op te zetten met behulp van quantum key distribution (QKD), waardoor langdurige bescherming tegen quantumdreigingen wordt gewaarborgd (digital-strategy.ec.europa.eu)

Ondersteuning voor crypto-agility

PQC-handboek - Evalueer en plan een naadloze migratie naar post-quantumcryptografische systemen (aivd.nl)

IMPACT

Onderwijs

- Post-quantumbeveiligingsinbreuken zijn mogelijk vanwege open IT-omgevingen, afhankelijkheid van externe cloudproviders en het langdurig bewaren van vertrouwelijke data.
- Identiteiten van bijvoorbeeld studenten kunnen in gevaar komen door de openbaarmaking van cijferlijsten, beoordelingen of persoonlijke informatie.
- Gearchiveerde lesmaterialen, communicatie of certificeringsgegevens kunnen worden vervalst of gewijzigd.

Onderzoek

- “Nu opslaan, later ontsleutelen” vormt een aanzienlijke bedreiging voor de vertrouwelijkheid van onderzoek. Informatie zoals genetische data en AI-modellen die vandaag wordt onderschept en opgeslagen, kan later worden ontsleuteld, met risico op blootlegging van vertrouwelijke of bedrijfsgevoelige informatie.
- Onderzoekspartners kunnen aarzelen om gegevens te delen of samen te werken als er quantumonveilige systemen worden gebruikt, wat kan leiden tot een verstoring van de op vertrouwen gebaseerde samenwerking.
- Universiteiten die betrokken zijn bij octrooieerbaar of commercieel relevant onderzoek kunnen hun concurrentievoordeel verliezen in geval van diefstal van intellectueel eigendom.
- Het niet beveiligen van gegevens kan leiden tot beperkingen van financieringsinstanties of niet-naleving van ethische en wettelijke vereisten.

Operations

Het opkomende risico dat quantumcomputers uiteindelijk de huidige versleutelingsalgoritmen zullen kraken, zet staatsactoren er nu al toe aan om data met een langdurige gevoeligheid op te slaan en later te ontsleutelen. Daarom moet er een belangrijke PQC-infrastructuur worden opgezet. Zonder vroegtijdige PQC-maatregelen op het gebied van beleid en infrastructuurfinanciering lopen instellingen het risico dat hun data op lange termijn worden blootgesteld en dat het vertrouwen wordt ondermijnd.

TREND #4

Opkomst van maat-regelen voor veilige internet-of-things-omgevingen

Publieke waarden

Autonomie	Privacy
Rechtvaardigheid	Rekenschap | Integriteit
Menselijkheid	Veiligheid

Volwassenheid WATCH PLAN **ACT**

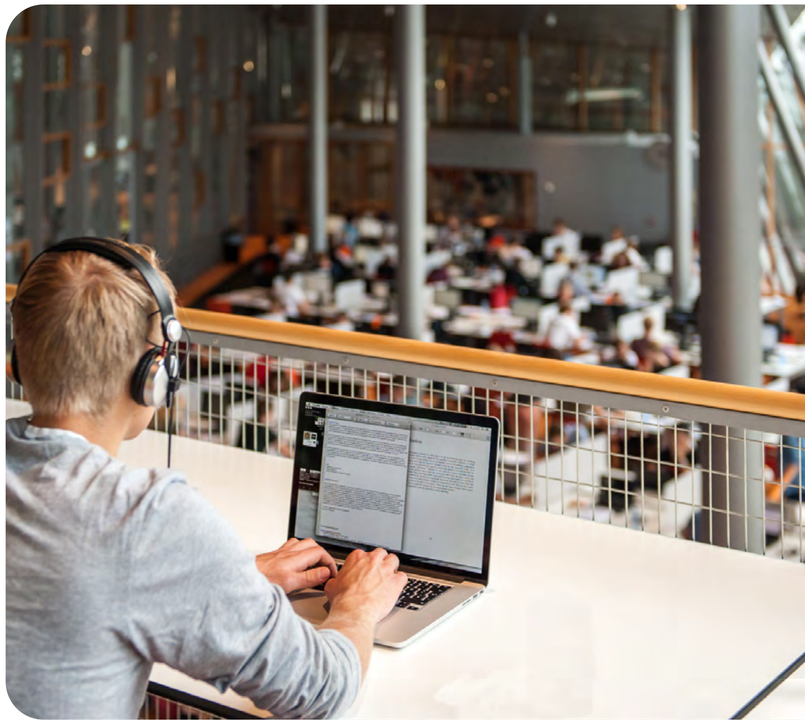
Drivers

Connectiviteit en interactie; Cybersecurity en vertrouwen; Digitale transformatie; Regelgeving en naleving (compliance); Kritieke infrastructuur; Individualisering en empowerment

Het internet-of-things (IoT) is niet meer weg te denken en zorgt voor een revolutie in verschillende sectoren door de efficiëntie te verbeteren en meer inzichten te bieden. Toch brengt het ook aanzienlijke veiligheids-uitdagingen en risico's met zich mee, bij-voorbeeld op het gebied van identificatie, authenticatie en eigendom van 'slimme' apparaten, zoals autonome drones.

De afgelopen 10 jaar hebben ontwikkelaars en leveranciers van IoT hun verantwoorde-lijkheid voor beveiligingsupdates gedurende de levensduur van producten verwaarloosd, wat cybersecurity-kwestsbaarheden heeft gecreëerd binnen organisaties.

Om dergelijke risico's te beperken, worden beveiligingsoplossingen ontwikkeld, zoals endpointbescherming. Daarnaast zal nieuwe wetgeving, zoals de Cyber Resilience Act, IoT-ontwikkelaars en -leveranciers verplichten om gedurende de hele levensduur van een product beveiligingsupdates te verstrekken.



SIGNALEN

IoT-apparaten worden geïntegreerd in de dagelijkse praktijk

IoT-apparaten zijn te vinden en nemen toe in alle verticale markten en toeleveringsketens, in hun integratie in dagelijkse praktijken, of het nu in het ziekenhuis, de fabriek of thuis is (demandsage.com)

De EU-wet inzake cyberweerbaarheid (CRA) van kracht vanaf 2024 (digital-strategy.ec.europa.eu)

IoT-beveiliging heeft zijn eigen specifieke beveiliging

Een overzicht van meervoudige authenticatie in internet of healthcare things (doi.org)

UTwente heeft een IoT Cyberlab geopend (utwente.nl)

Edge AI: cloud en apparaten verbinden voor veilige, duurzame AI (doiotfieldlab.tudelftcampus.nl)

Praktische maatregelen en richtlijnen

Tips van het Nationaal Cyber Security Centrum (ncsc.nl)

Richtlijnen voor het beveiligen van het internet-of-things (enisa.europa.eu)

IMPACT

Onderwijs

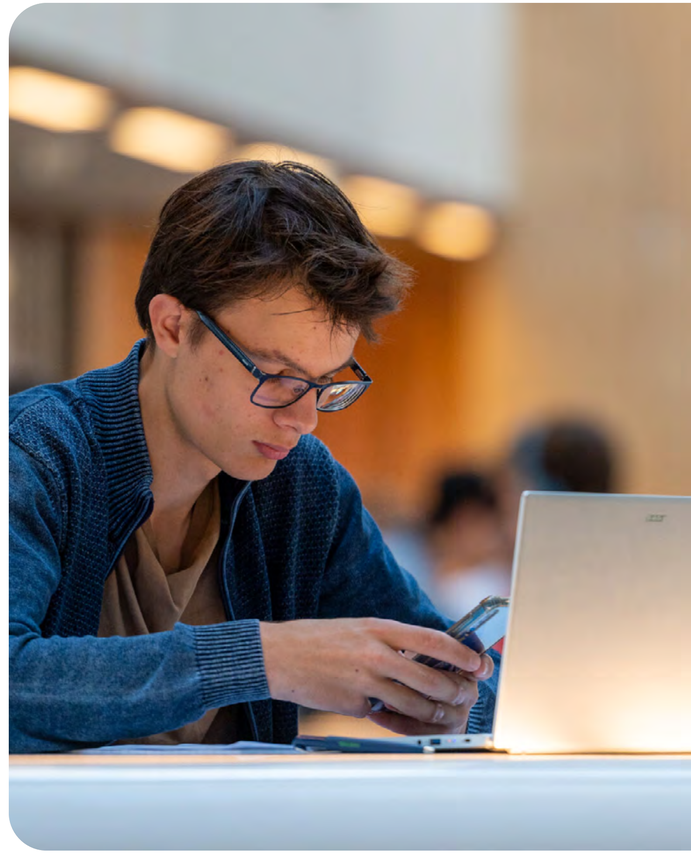
Beroepsopleidingen zoals system-engineering integreren IoT en de beveiligingsaspecten ervan in het curriculum. De toepassing van IoT in onderwijsmethoden richt zich echter minder op digitale technologie, zoals het geven van directe feedback. Het mogelijk maken van gepersonaliseerd leren blijft beperkt.

Onderzoek

- De veilige implementatie van IoT kan ook bijdragen aan het verzamelen van data voor wetenschappelijk onderzoek (bijvoorbeeld via apparaten en wearables).
- IoT en de beveiliging van IoT worden onderzocht in een breed scala aan toepassingen bij onderzoeksinstellingen. Dit omvat bijvoorbeeld privacybeschermende en veilige protocollen voor wearables in de gezondheidszorg, slimme verkeersbeheersystemen en de ontwikkeling van modellen die IoT-aanvallen detecteren en classificeren.

Operations

IoT wordt vaak over het hoofd gezien door IT-beveiligingsdiensten, ondanks de aanzienlijke toename van het aanvalsoppervlak (kwetsbare plekken waarop cyberaanvallen kunnen plaatsvinden). Het is van belang dat IT-securityteams grip krijgen op hun (verborgen) IoT-assets, veilig gebruik van IoT stimuleren en medewerkers en studenten informeren over de risico's van IoT. Instellingen wordt aangeraden om IoT-netwerken te isoleren, speciale servers te gebruiken en governancekaders te implementeren om een veilige invoering van IoT te waarborgen.



TREND #5

Het groeiende belang van beveiligings-protocollen voor het werken in de cloud

Publieke waarden

Autonomie	Privacy
Rechtvaardigheid	Integriteit | Rekenschap | Transparantie
Menselijkheid	Veiligheid

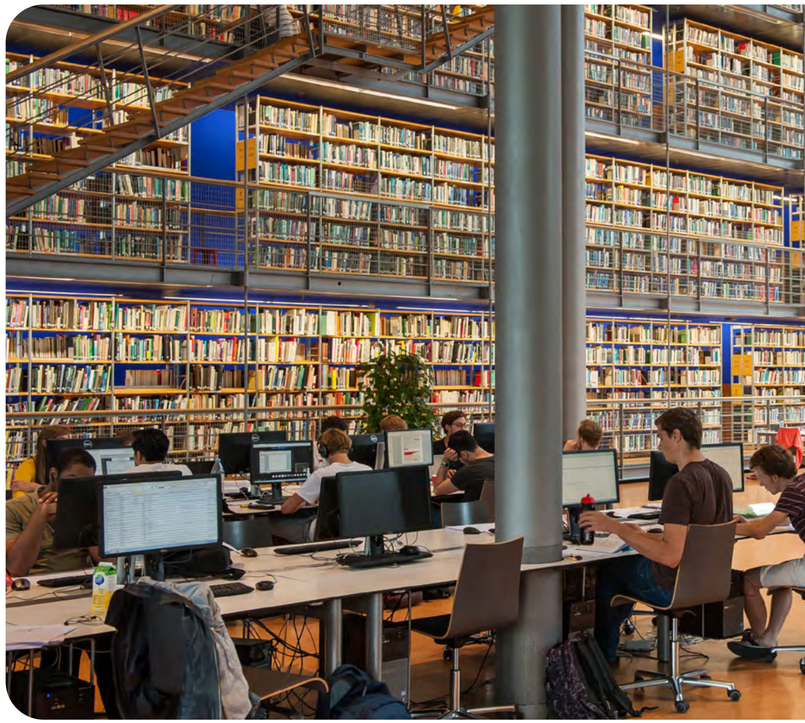
Volwassenheid WATCH PLAN ACT

Drivers

Automatisering en AI; Technologische vooruitgang en computation; Cybersecurity en vertrouwen; Digitale transformatie; Dienstgerichte en waardegedreven economieën; Belang van kennis en vaardigheden

Cloud computing maakt uitzonderlijke schaalbaarheid, flexibiliteit en kostenbesparing mogelijk. Toch leidt de wijdverspreide inzet van cloudservices tot aanzienlijke beveiligingsrisico's. Deze hebben te maken met gedeelde verantwoordelijkheden tussen cloudproviders en -gebruikers, een vergroot aanvalsoppervlak, afhankelijkheid van externe dienstverleners (toeleveranciers) en onvoldoende transparantie in de gebruikte software en hardware.

Bovendien maakt AI-integratie beveiligings- en privacykwesties complexer. Hybride cloudopstellingen vereisen robuuste beveiligingsmaatregelen, zoals zero-trustaanpak (met nadruk op voortdurende authenticatie en beperkte toegang tot netwerkbronnen), continue monitoring en krachtige encryptie.



SIGNALEN

Europese en nationale alternatieven voor clouddiensten

Start Next Cloud-pilot: zeventig onderzoekers van vijf Nederlandse universiteiten (communities.surf.nl)

Vijf Nederlandse universiteiten experimenteren met alternatieve Europese cloudoplossingen (voxweb.nl)

Nederlandse overheid zet in op Nederlandse soevereine cloud voor gevoelige informatie

- security.nl
- open.overheid.nl)

EU FED Cloud, die voldoet aan relevante EU-regelgeving zoals de Data Act, AI Act, GDPR, eIDAS, DORA en EUCS (eufedcloud.eu)

EOSC EU Node (open-science-cloud.ec.europa.eu)

Europese juridische ontwikkelingen

NIS2-richtlijn van kracht, ook in het hoger onderwijs (bedrijfsleven.nl)

EU-verordening Cyber Resilience Act (CRA) (eur-lex.europa.eu)

IMPACT

Onderwijs

- De manier waarop gewerkt wordt met cloudcomputingtechnologieën ontwikkelt zich voortdurend. Het gaat daarbij bijvoorbeeld om het wisselen tussen cloudproviders en -oplossingen, meer aandacht voor cybersecurity en het belang van datasoevereiniteit en soevereiniteit in bredere zin. Dergelijke onderwerpen krijgen steeds meer een plek in onderwijsprogramma's.
- Aanpassingen in IT-opleidingsprogramma's kunnen helpen om de cruciale vaardigheden van cybersecurityprofessionals te versterken.

Onderzoek

- Door het tekort aan cybersecurityprofessionals blijven onderzoekomgevingen kwetsbaar voor cyberdreigingen, wat de integriteit van onderzoeksprocessen en -resultaten kan aantasten. Om dit te beperken, kan worden onderzocht hoe cybersecuritybewustzijnstrainingen voor onderzoekers kunnen worden ingezet.
- Gedeelde verantwoordelijkheden kunnen leiden tot datalekken of gegevensverlies, vooral als onderzoekers niet op de hoogte zijn van beveiligingsprotocollen.
- Onderzoekers moeten zich houden aan verschillende voorschriften met betrekking tot gegevensbescherming en privacy, wat door de cloudomgeving nog ingewikkelder kan worden.

Operations

- Naarmate instellingen steeds meer cloudoplossingen inzetten, wordt zorgvuldige planning en versterkte beveiliging essentieel om gevoelige gegevens te beschermen, compliance te waarborgen en de weerbaarheid tegen dreigingen te behouden. Ook de impact van data- en systeemmigraties zal groot zijn. Bovendien wordt verwacht dat het gebruik van open-source software (OSS) verder zal groeien.
- Hoewel hybride cloudomgevingen flexibiliteit bieden, vereisen ze geavanceerde beveiligingsmaatregelen, die voor sommige onderzoeksinstellingen moeilijk effectief te implementeren kunnen zijn.

Meer informatie over cybersecurity? Bezoek surf.nl

SURF Utrecht
Kantoren Hoog Overborch
Hoog Catharijne
Moreelsepark 48
3511 EP Utrecht
+31 88 787 30 00

SURF Amsterdam
Science Park 140
1098 XG Amsterdam
+31 88 787 30 00

futuring@surf.nl
www.surf.nl